

REMARKS

Amendments

Claims 1 and 10 have been amended to more clearly recite the subject matter for which protection is sought to avoid any misinterpretation of the original claim language. Thus, claim 1 is amended to recite that the portable data carrier is arranged to perform different user authentication methods and describes the manner in which quality information regarding authentication of the user is carried out by the portable data carrier to determine proof of authentication. Support for the amendment is found, for example, at page 2, paragraph 3 and page 5, paragraph 1 of the specification.

Claim 10 has been amended in a manner so that it is consistent with claim 1 and support for the amendment is found in the same locations within the written description as identified above with respect to the amendments made to claim 1.

Claim Objections

The objections to claims 1, 10 and 14 are moot in view of the amendments made to the claims.

Claim Rejections – 35 USC §112

The rejection of claims 1 and 10 under 35 USC §112 is now moot in view of the amendments made to the claims. The word “locating” in claims 1 and 10 was a typographical error. The term “creating” was the intended word to be used in the claims.

Claim Rejections – 35 USC §102

The rejection of claims 1, 3-8, 10, 12 and 14 under 35 USC §102(e) on grounds that the claims are anticipated by Mimura (U.S. 7,162,058) is now moot in view of the amendments made to claims 1 and 10. Specifically, the original step in claim 1 of creating quality information about how the user has been authenticated has been expanded somewhat to provide a better foundation for the process of developing quality information regarding the authentication procedure that is used by the portable data carrier. More specifically, as described in the specification, the portable data carrier is arranged to perform *different user authentication methods*, and then, the data carrier performs a security-establishing operation

comprising creating quality information about how the authentication of the user was performed *by the used user authentication method*.

Clearly, there is not the remotest suggestion in Mimura that different authentication procedures can be used by the user or creating quality information via the authentication program described in the patent. On the contrary, Mimura simply teaches a fingerprint comparison authentication process and nothing more to establish authentication by a user.

As explained in the specification, the problem solved by the present invention lies in effecting a secure electronic transaction using a portable data carrier which takes into account the quality of the user authentication performed. When the user authentication is being performed in accordance with the invention, the performing data carrier produces quality information about the authentication procedure used. This "voucher" is attached to the result of a security-establishing operation subsequently performed by the portable data carrier. The recipient of the thus formed message can therefore clearly recognize how a user has authenticated himself before effecting the security-establishing operation. Accordingly, a secure transaction can be affected contingent on the quality of the user authentication.

For example, in an electronic purse application, authentication for an application involving the withdrawal of a sum of money below a limiting value can be effected after a simple PIN authentication, while amounts of money to be withdrawn above such limiting value would require a more secure authentication, such as by means of a biometric feature. (See page 2, first paragraph.)

The result is that tampering with an authentication voucher even when an authorized user has access to both a portable data carrier and an associated, low-order authentication information, is rendered virtually impossible, even though the user has an associated PIN. (See page 2, third paragraph.) This is quite different from Mimura, where the electronic authentication unit compares a fingerprint image of a clerk with a reference fingerprint information stored on the IC card 100, with the authentication unit 103 performing an electronic authentication with a host computer 130 if the fingerprints match. If the newly inputted fingerprint matches the reference fingerprint information 104, access to the authentication information 105 is allowed and the authentication is made between the applications 131 and the electronic authentication unit 103 so that the access from the terminal 120 to the applications 130 is permitted, enabling the clerk to authorize the application.

As noted previously, nothing is disclosed in Mimura regarding the availability of multiple authentication procedures in combination with the creation of quality information by a portable data carrier about how an authentication of the user was performed, followed by using such information during the security-establishing operation.

Accordingly, it is respectfully submitted that withdrawal of the rejection of claim 1 is in order and the same is respectfully requested.

The above remarks apply equally with regard to apparatus claim 10. The withdrawal of the rejection of claim 10 is likewise requested.

Claims 2-9 and 11-14 are patentable at least on the basis of the patentability of claims 1 and 10 from which they depend. In addition, each claim recites additional subject matter that further distinguishes the elements of the independent claims over the cited prior art. Accordingly, allowance of the dependent claims 2-9 and 11-14 is in order and the same is requested.

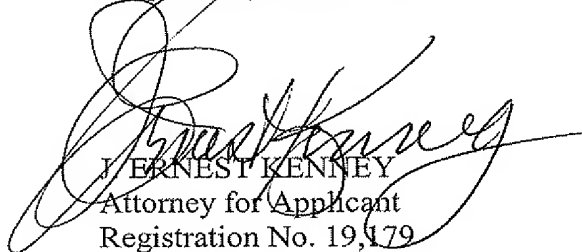
Claim Rejections – 35 USC §103

The rejection of claims 2 and 11 under 35 USC §103(a) in view of Mimura and Barlow is moot in view of the amendments to the claims and it is respectfully submitted that the patentability of claims 2 and 11 has been established by the amendments to claims 1 and 10, and likewise, with regard to claims 9 and 13.

The application having been placed in condition for allowance, its passage to issue is respectfully requested.

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, VA 22314-1176
Phone: (703) 683-0500
Facsimile: (703) 683-1080
Date: November 26, 2008

Respectfully submitted,


J. ERNEST KENNEY
Attorney for Applicant
Registration No. 19,179